Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 5 (2016), pp. 4253–4271

http://www.ripublication.com/gjpam.htm

On Elements of Split Quaternions over $\mathbb{Z}_p$

Shin Min Kang

Department of Mathematics and RINS,
Gyeongsang National University,
Jinju 52828, Korea.

Mobeen Munir

Division of Science and Technology,
University of Education,
Lahore 54000, Pakistan.

Abdul Rauf Nizami

Division of Science and Technology,
University of Education,
Lahore 54000, Pakistan.

Muazzam Ali

Division of Science and Technology,
University of Education,
Lahore 54000, Pakistan.

Waqas Nazeer[1]

Division of Science and Technology,
University of Education,
Lahore 54000, Pakistan.

[1]Corresponding author.

Abstract

The aim of this work is to highlight some key differences in the algebras of quaternions and split quaternions over $\mathbb{Z}_p$ for some prime p. We actually give closed formulas for the number of idempotents, nilpotents, and zero divisors that are common in both algebras.

AMS subject classification: 11R52.
Keywords: Split quaternion, Idempotents, Nilpotents, Zero divisors.

1. Introduction

Split quaternions were introduced by Cockle in 1849 in [8]. Split quaternions plays a vital role in geometry and physical models in 4-dimensional space. Split quaternions are used to express Lorentzian rotations [6, 15, 19]. Particularly, the geometric and physical applications of split quaternions require solving split quaternionic equations [1, 10].

Recently, Kula and Yayli [15] showed that algebra of split quaternions $\mathbb{H}_s$ has a scalar product that identifies it with semi-Euclidean space $\mathbb{E}_2^4$. Özdemir [17] expressed Euler's and De Moivre's formula for split quaternions and examined roots of split quaternions with respect to causal character of split quaternions. For detailed information of split quaternions, we refer the reader to [5, 9, 12, 13, 14, 18].

Initially, the ring of quaternions over $\mathbb{Z}_p$ was studied by Aristidou and Demetre in [4], who showed that the Kandasamy's theorem regarding finite ring $\mathbb{H}/\mathbb{Z}_p$ is false. Moreover, he showed that the set $\mathbb{H}/\mathbb{Z}_p$ does not form a finite skew field as it contains zero divisors. In [2], Aristidou discussed the idempotents in $\mathbb{H}/\mathbb{Z}_p$. In [16], Miguel gave more detailed structure of $\mathbb{H}/\mathbb{Z}_p$, in particular, he discussed the zero divisors. He also gave the formula for the number of idempotents and zero divisors in $\mathbb{H}/\mathbb{Z}_p$. Aristidou [3] discussed the nilpotents in $\mathbb{H}/\mathbb{Z}_p$. He gave the condition of nilpotency index $\mathbb{H}/\mathbb{Z}_p$ and proved that there are p^2 nilpotent elements in it.

This paper characterizes mainly the idempotents, nilpotents, and zero divisors in the algebras of quaternions and split quaternions.

To avoid confusion, we shall use the notations $\mathbb{H}/\mathbb{Z}_p$ for the algebra of quaternions and $\mathbb{H}_s/\mathbb{Z}_p$ for the algebra of split quaternions. Moreover, by $Id(R)$, $nil(R)$, and $Zd(R)$ we shall mean the sets of idempotents, nilpotents, and zero divisors in the ring R.

Definition 1.1. *Split-quaternion algebra* $\mathbb{H}_s$ is an associative, non-commutative, and non-division ring with four basic elements $\{1, i, j, k\}$ with conditions:

$$i^2 = -1, \quad j^2 = k^2 = 1, \quad ij = k = -ji,$$
$$jk = -i = -kj, \quad ki = j = -ik, \quad ijk = 1.$$

A typical element x of this algebra is of the form $q_0 + q_i + q_2 j + q_3 k$, where $q_0, q_1, q_2, q_3 \in \mathbb{Z}_p$. The *conjugate* of x is defined as

$$\overline{x} = q_0 - q_1 i - q_2 j - q_3 k.$$

The *norm* of x denoted as $N(x)$ is

$$N(x) = x\overline{x} = q_0^2 + q_1^2 - q_2^2 - q_3^2.$$

It is easy to see that for any $x \in \mathbb{H}_s/\mathbb{Z}_p$ the relation $x^2 - 2q_0x + N(x) = 0$ holds.

Definition 1.2. An element x of a ring R is *idempotent* if $x^2 = x$ and is *nilpotent* if $x^m = 0$ for $m \in \mathbb{Z}^+$. A nonzero element x of R is called *zero divisor* if there exists a nonzero element y of R such that $xy = 0$ or $yx = 0$.

The main results are the following theorems.

Theorem 1.3. $\mathbb{H}_s/\mathbb{Z}_p \cong \mathbb{M}_2(\mathbb{Z}_p)$, where p is prime.

The condition for an element of $\mathbb{H}_s/\mathbb{Z}_p$ to be an idempotent is given in the theorem:

Theorem 1.4. Let $x = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}_s/\mathbb{Z}_p$, where p is an odd prime. If x is idempotent, then following statements hold:

(a) If $N(x) = 0$, then $q_0 = \dfrac{p+1}{2}$.

(b) x is idempotent if and only if $q_0 = \dfrac{p+1}{2}$ and $-q_1^2 + q_2^2 + q_3^2 = \dfrac{1-p^2}{4}$.

(c) x is idempotent if and only if $\overline{x}$ is also idempotent.

(d) If $p = 2$, then $x = q_0$.

Theorem 1.5. If p is an odd prime, then $\left|Id(\mathbb{H}_s/\mathbb{Z}_p)\right| = p^2 + p + 2$.

Theorem 1.6. If $x \in \mathbb{H}_s/\mathbb{Z}_p$ is nilpotent, then

(a) $N(x) = 0$.

(b) $q_0 = 0$.

(c) $x^2 = 0$.

Theorem 1.7. If $x \in \mathbb{H}_s/\mathbb{Z}_p$ is a nilpotent of index 2, then following statements hold:

(a) $x = q_i \pm q_1 j$.

(b) If $x = q_i \pm q_2 j + q_3 k$, then $q_1^2 = q_2^2 + q_3^2$.

Theorem 1.8. $\left|nil(\mathbb{H}_s/\mathbb{Z}_p)\right| = p^2$.

Theorem 1.9. If $x \in \mathbb{H}_s/\mathbb{Z}_p$, where p is an odd prime, then following statements hold:

(a) x is zero divisor if and only if $N(x) = 0$.

(b) If $q_0 = \dfrac{p \pm (2k+1)}{2}$ and $q_1^2 - q_2^2 - q_3^2 = \dfrac{p^2 - (2k+1)^2}{4}$, where $k \in \mathbb{Z}_p$, then x is a zero divisor.

Theorem 1.10. The number of zero divisors in $\mathbb{H}_s/\mathbb{Z}_p$ is $p^3 + p^2 - p$, where p is an odd prime.

The following theorems show the elements (idempotents, nilpotents, and zero divisors) that are common in $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$.

Theorem 1.11.

$$|Id(\mathbb{H}/\mathbb{Z}_p) \cap Id(\mathbb{H}_s/\mathbb{Z}_p)| = \begin{cases} 2 & \text{if } p = 2, \\ 2 & \text{if } p \equiv 3 \ (mod\, 4), \\ 4p & \text{if } p \equiv 1 \ (mod\, 4). \end{cases}$$

Theorem 1.12.

$$|nil(\mathbb{H}/\mathbb{Z}_p) \cap nil(\mathbb{H}_s/\mathbb{Z}_p)| = \begin{cases} 4 & \text{if } p = 2, \\ 1 & \text{if } p \equiv 3 \ (mod\, 4), \\ 2p-1 & \text{if } p \equiv 1 \ (mod\, 4). \end{cases}$$

Theorem 1.13.

$$|Zd(\mathbb{H}/\mathbb{Z}_p) \cap Zd(\mathbb{H}_s/\mathbb{Z}_p)| = \begin{cases} 8 & \text{if } p = 2, \\ 1 & \text{if } p \equiv 3 \ (mod\, 4), \\ (2p-1)^2 & \text{if } p \equiv 1 \ (mod\, 4). \end{cases}$$

2. Proofs

Proof Theorem 1.3. It is easy to see that $\mathbb{H}_s/\mathbb{Z}_p$ and $M_2(\mathbb{Z}_p)$, as algebras, are isomorphic; the map $\varphi : \mathbb{H}_s/\mathbb{Z}_p \to M_2(\mathbb{Z}_p)$ is defined as

$$\begin{aligned} &\varphi(q_0 + q_1 i + q_2 j + q_3 k) \\ &= q_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + q_1 \begin{pmatrix} 0 & p-1 \\ 1 & 0 \end{pmatrix} + q_2 \begin{pmatrix} 0 & p-1 \\ p-1 & 0 \end{pmatrix} + q_3 \begin{pmatrix} p-1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

First we prove its bijection: If we consider $\mathbb{H}_s/\mathbb{Z}_p$ and $M_2(\mathbb{Z}_p)$ as 4-dimensional space, then φ is a linear mapping. The coefficient matrix of the homogeneous system $\varphi(q_0 + q_1 i + q_2 j + q_3 k) = 0$ is

$$R = \begin{pmatrix} 1 & 0 & 0 & p-1 \\ 0 & p-1 & p-1 & 0 \\ 0 & 1 & p-1 & 0 \\ 1 & 0 & 0 & p-1 \end{pmatrix}.$$

Since $|R| \neq 0$, φ is bijective.

Note that

$$\begin{aligned}\varphi(x+y) &= (q_0+q_0')\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + (q_1+q_1')\begin{pmatrix}0 & p-1\\ 1 & 0\end{pmatrix}\\ &\quad + (q_2+q_2')\begin{pmatrix}0 & p-1\\ p-1 & 0\end{pmatrix} + (q_3+q_3')\begin{pmatrix}p-1 & 0\\ 1 & 1\end{pmatrix}\\ &= \varphi(x)+\varphi(y).\end{aligned}$$

Now the relation $\varphi(xy)=\varphi(x)\varphi(y)$ is clear from the relations

$$\begin{aligned}\varphi(xy) &= (q_0q_0' - q_1q_1' + q_2q_2' + q_3q_3')\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ &\quad + (q_0q_1' + q_1q_0' - q_2q_3' + q_3q_2')\begin{pmatrix}0 & p-1\\ 1 & 0\end{pmatrix}\\ &\quad + (q_0q_2' + q_2q_0' + q_3q_1' - q_1q_3')\begin{pmatrix}0 & p-1\\ p-1 & 0\end{pmatrix}\\ &\quad + (q_0q_3' + q_1q_2' - q_2q_1' + q_3q_0')\begin{pmatrix}p-1 & 0\\ 0 & 1\end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}\varphi(x)\varphi(y) &= \varphi(q_0+q_1i+q_2j+q_3k)\varphi(q_0'+q_1'i+q_2'j+q_3'k)\\ &= \left[q_0\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + q_1\begin{pmatrix}0 & p-1\\ 1 & 0\end{pmatrix} + q_2\begin{pmatrix}0 & p-1\\ p-1 & 0\end{pmatrix} + q_3\begin{pmatrix}p-1 & 0\\ 1 & 1\end{pmatrix}\right]\\ &\quad \times\left[q_0'\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + q_1'\begin{pmatrix}0 & p-1\\ 1 & 0\end{pmatrix} + q_2'\begin{pmatrix}0 & p-1\\ p-1 & 0\end{pmatrix} + q_3'\begin{pmatrix}p-1 & 0\\ 1 & 1\end{pmatrix}\right]\\ &= (q_0q_0' - q_1q_1' + q_2q_2' + q_3q_3')\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ &\quad + (q_0q_1' + q_1q_0' - q_2q_3' + q_3q_2')\begin{pmatrix}0 & p-1\\ 1 & 0\end{pmatrix}\\ &\quad + (q_0q_2' + q_2q_0' + q_3q_1' - q_1q_3')\begin{pmatrix}0 & p-1\\ p-1 & 0\end{pmatrix}\\ &\quad + (q_0q_3' + q_1q_2' - q_2q_1' + q_3q_0')\begin{pmatrix}p-1 & 0\\ 0 & 1\end{pmatrix}.\end{aligned}$$

This completes the proof. ∎

In the following, we give shall give the condition for an element to be idempotent in $\mathbb{H}_s/\mathbb{Z}_p$. Then we shall give some characterizations of the idempotent elements. At the end we shall give number of idempotents in $\mathbb{H}_s/\mathbb{Z}_p$.

Proof for Theorem 1.4.

(a) Suppose that x is a nonzero idempotent. Then, as $x^2 = 2q_0x - N(x)$, we have $x = 2q_0x - N(x)$ or $N(x) = (2q_0 - 1)x$. If $N(x) = 0$, then $q_0 = \frac{p+1}{2}$.

(b) If x is a nontrivial idempotent, then from the relation $2q_0x - N(x) = x$ we get

$$2q_0^2 + 2q_0q_1i + 2q_0q_2j + 2q_0q_3k - q_0^2 - q_1^2 + q_2^2 + q_3^2 = q_0 + q_1i + q_2j + q_3k.$$

From here we receive the equations:

$$q_0^2 - q_1^2 + q_2^2 + q_3^2 = q_0,$$

$$2q_0q_1 = q_1, 2q_0q_2 = q_2,$$

and $2q_0q_3 = q_3$. It now follows that either $q_1 = 0$ or $q_0 = \frac{1}{2}$. Since p is an odd prime, $q_0 = \frac{p+1}{2}$. Now

$$\left(\frac{p+1}{2}\right)^2 - q_1^2 + q_2^2 + q_3^2 = \frac{p+1}{2}$$

or

$$-q_1^2 + q_2^2 + q_3^2 = \frac{1-p^2}{4}.$$

Conversely,

$$x^2 = 2q_0x - N(x) = 2\left(\frac{p+1}{2}\right)x - \left(\frac{p+1}{2}\right)^2 + \frac{p^2-1}{4} = x.$$

(c) If $\overline{x}$ is idempotent, then $\overline{x}^2 = \overline{x}$ or $2q_0\overline{x} - N(\overline{x}) = \overline{x}$ or

$$2q_0^2 - 2q_0q_1i - 2q_0q_2j - 2q_0q_3k - q_0^2 - q_1^2 + q_2^2 + q_3^2 = q_0 - q_1i - q_2j - q_3k.$$

Comparing the coefficients, we get

$$q_0^2 - q_1^2 + q_3^2 + q_3^2 = q_0,$$

$$2q_0q_1 = q_1, 2q_0q_2 = q_2,$$

and $2q_0q_3 = q_3$. It follows that $q_0 = \frac{p+1}{2}$ and

$$-q_1^2 + q_2^2 + q_3^2 = \frac{1-p^2}{4}.$$

So, if $x \in \mathbb{H}_s/\mathbb{Z}_p$ is idempotent if and only if $\overline{x}$ is idempotent.

(d) If $p = 2$, the only possibility is that $q_1 = q_2 = q_3 = 0$. So $x = q_0$. Now from the relation $q_0^2 = q_0$ or $q_0(q_0 - 1) = 0$ it follows that either $x = 0$ or $x = 1$. ■

Proof for Theorem 1.5. Since $\mathbb{H}_s/\mathbb{Z}_p \cong M_2(\mathbb{Z}_p)$, $|Id(\mathbb{H}_s/\mathbb{Z}_p)| = |Id(M_2(\mathbb{Z}_p))|$. A matrix $M_2(\mathbb{Z}_p)$ is idempotent if $M^2 = M\ (mod\ p)$ or $M(M - I) = 0\ (mod\ p)$. For instance, if

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a-1 & b \\ c & d-1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Case 1. If $b = c = 0$, then we get $a(a-1) \equiv 0(\mod p)$ and $d(d-1) \equiv 0\ (mod\ p)$. It follows that each of a and d has two solutions, 0 and 1.

Case 2. If $b \equiv 0\ (mod\ p)$ but $c \not\equiv 0\ (mod\ p)$, then $a(a-1) \equiv 0 (\mod p)$, $d(d-1) \equiv 0\ (mod\ p)$, and $c(a + d - 1) \equiv 0\ (mod\ p)$. Again, a and d receive 0 and 1; however, c takes $p - 1$ values. So, there are $2(p - 1)$ matrices satisfying these relations.

Case 3. If $b \not\equiv 0\ (mod\ p)$ and $c \equiv 0\ (mod\ p)$, then, again, $2(p - 1)$ matrices appear.

Case 4. If $b \not\equiv 0\ (mod\ p)$ and $c \not\equiv 0\ (mod\ p)$, then we receive the following four relations $a^2 - a + bc \equiv 0 (\mod p)$, $b(a + d - 1) \equiv 0\ (mod\ p)$, $c(a + d - 1) \equiv 0\ (mod\ p)$, and $d^2 - d + bc \equiv 0 (\mod p)$. It follows that $a + d \equiv 0 (\mod p)$, where a and d can not take 0 and 1 as it leads to $bc = 0$, which is a contradiction. So, there are $p - 2$ possibilities for a and d, and there are $p - 1$ choices for both b and c. So, there are $(p - 2)(p - 1)$ total possible matrices of this form. Adding all the above possibilities from all the cases, we get

$$4 + 2(p - 1) + 2(p - 1) + (p - 2)(p - 1) = p^2 + p + 2.$$

This completes the proof. ■

Proof for Theorem 1.6. $(b) \Rightarrow (a)$. Since $x^2 - 2q_0x + N(x) = 0$, we must have $x^2 = -N(x)$. It follows from the relation $(x^2)^m = (-N(x))^m$ that $0 = (-1)^m(N(x))^m$, which further implies that $N(x) = 0$.

$(a) \Rightarrow (b)$. **Case 1.** (When m is odd) Let m be the nilpotency index. Then $x^2 = 2q_0x$ or $(x^2)^{\frac{m+1}{2}} = (2q_0x)^{\frac{m+1}{2}}$ or $x.x^m = (2q_0)^{\frac{m+1}{2}}x^{\frac{m+1}{2}}$. So $q_0 = 0$.

Case 2. (When m is even) Similarly $(x^2)^{\frac{m}{2}} = (2q_0x)^{\frac{m}{2}}$ implies $q_0 = 0$. ■

Proof for Theorem 1.7.

(a) If $x = q_1i \pm q_1j$, then, for $m = 2$, we have $x^2 = -q_1^2 + q_1^2k - q_1^2k + q_1^2 = 0$.

(b) If $x = q_1i + q_2j + q_3k$ then $x^2 = 0$. ■

Proof for Theorem 1.8. As $\mathbb{H}_s/\mathbb{Z}_p \cong \mathbb{M}_2(\mathbb{Z}_p)$, $|nil(\mathbb{H}_s/\mathbb{Z}_p)| = |nil(\mathbb{M}_2(\mathbb{Z}_p))|$. In [11], Fine and Herstein showed that the probability that $n \times n$ matrix over a Galois field having p^{α} elements having $p^{-\alpha \cdot n}$ nilpotent elements. As, in our case, $\alpha = 1$ and $n = 2$, the probability that 2×2 matrix over $\mathbb{Z}_p$ is nilpotent is p^{-2}. So,

$$\frac{|nil(M_2(\mathbb{Z}_p))|}{|(M_2(\mathbb{Z}_p)|} = p^{-2}$$

or $|nil(M_2(\mathbb{Z}_p))| = p^2$. ■

Proof for Theorem 1.9. (a) Suppose that x is a zero divisor. Then there exists a nonzero y such that $xy = 0$, $\overline{x}xy = 0$, and $N(x)y = 0$. So $N(x) = 0$.

Conversely, suppose that $N(x) = 0$. Then $x\overline{x} = 0$. This means that x is a zero divisor.

(b) If $x = q_0 + q_1 i + q_j + q_k$, then

$$\begin{aligned} x\overline{x} &= q_0^2 - q_0q_1i - q_0q_2j - q_0q_3k + q_0q_1i + q_1^2 - q_2q_2i \cdot j - q_1q_3j \cdot k \\ &\quad + q_0q_2j - q_1q_2j \cdot i - q_2^2 - q_2q_3j \cdot k + q_0q_3k - q_1q_3k \cdot i - q_2q_3k \cdot j - q_3^2 \\ &= q_0^2 + q_1^2 - q_2^2 - q_3^2. \end{aligned}$$

If $q_0 = \dfrac{p + (2k+1)}{2}$ and $q_1^2 - q_2^2 - q_3^2 = \dfrac{p - (2k+1)^2}{4}$, then $x\overline{x} = 0$.

Similarly, if $x\overline{x} = 0$, then $q_0 = \dfrac{p - (2k+1)}{2}$ and

$$q_1^2 - q_2^2 - q_3^2 = \frac{p^2 - (2k+1)^2}{4}.$$

■

Proof for Theorem 1.10. Here we also find the the number of zero divisors of $M_2(\mathbb{Z}_p)$. A matrix $S = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ is a zero divisor matrix if and only if it is a singular matrix. So, $ru - st = 0(modp)$. Thus the number of zero divisors of $\mathbb{H}_s/\mathbb{Z}_p$ is the same as the number of solutions of above equation are in $\mathbb{Z}_p$.

Case 1. If $r \neq 0$, and s, t and u are fixed, then the equation $ry = st(modp)$ has $p^2(p-1)$ solutions. So, there are $p^2(p-1)$ singular matrices.

Case 2. If $r = 0, t \neq 0, s \neq 0$, then S is singular if and only if $st = 0(modp)$. There are $p - 1$ such solutions of the above equation. Hence there are $p(p-1)$ singular matrices.

Case 3. Now if $r = t = 0$, then there are p^2 singular matrices. Thus the total number of zero divisors in $\mathbb{H}_s/\mathbb{Z}_p$ is $p^3 + p^2 - p$. ■

3. A comparison on the elements of $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$

In this section we reveal our main story. By the the computer codes, given in appendix, we list idempotents, nilpotents, and zero divisors. The tables generated from these codes lead us to draw some nice conclusions about $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$.

3.1. Comparison of idempotents

Case 1. For $p = 2$ the number of idempotents in both $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$ is 2, and are 0, 1.

Case 2. For $p = 3$, we get, from Theorem 1.4, that $q_0 = 2$ for both $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$, and $q_1^2 + q_2^2 + q_3^2 = 2$ in $\mathbb{H}/\mathbb{Z}_p$ and $-q_1^2 + q_2^2 + q_3^2 = 1$ in $\mathbb{H}_s/\mathbb{Z}_p$. Following table gives the values of q_1, q_2, and q_3, respectively, satisfying these relations.

$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$
0, 0, 1	0, 1, 1	1, 2, 2	1, 1, 0
0, 1, 0	0, 1, 2	2, 1, 1	1, 2, 0
0, 2, 0	0, 2, 1	2, 1, 2	2, 0, 1
0, 0, 2	0, 2, 2	2, 2, 1	2, 0, 2
1, 1, 1	1, 0, 1	1, 2, 1	2, 1, 0
2, 2, 2	1, 0, 2	1, 1, 2	2, 2, 0

Case 3. For $p = 5$, we have $q_0 = 3$, $-q_1^2 + q_2^2 + q_3^2 = 4$, and $q_1^2 + q_2^2 + q_3^2 = 1$.

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 2	0, 0, 1	1, 2, 4	1, 2, 4	3, 3, 2	3, 4, 1
0, 0, 3	0, 0, 4	1, 3, 4	1, 3, 4	3, 3, 3	3, 4, 4
0, 2, 0	0, 1, 0	1, 4, 2	1, 4, 2	4, 1, 2	4, 1, 2
0, 3, 0	0, 4, 0	1, 4, 3	1, 4, 3	4, 1, 3	4, 1, 3
1, 0, 0	1, 0, 0	2, 2, 2	2, 1, 1	4, 2, 1	4, 2, 1
4, 0, 0	4, 0, 0	2, 2, 3	2, 1, 4	4, 2, 4	4, 2, 4
1, 1, 2	1, 1, 2	2, 3, 2	2, 4, 1	4, 3, 1	4, 3, 1
1, 1, 3	1, 1, 3	2, 3, 3	2, 4, 4	4, 3, 4	4, 3, 4
1, 2, 1	1, 2, 1	3, 2, 2	3, 1, 1	4, 4, 2	4, 4, 2
1, 3, 1	1, 3, 1	3, 2, 3	3, 1, 4	4, 4, 3	4, 4, 3

The following theorem gives the number of idempotent elements that are common in both $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$ for a particular class of primes.

Proof for Theorem 1.11. **Case 1.** $(p = 2)$ If $x \in \mathbb{H}/\mathbb{Z}_p$, then

$$x^2 = q_0^2 - q_1^2 - q_2^2 - q_3^3 + 2q_0(q_1 i + q_2 j + q_3 k),$$

and if $x \in \mathbb{H}_s/\mathbb{Z}_p$ then

$$x_s^2 = q_0^2 - q_1^2 + q_2^2 + q_3^3 + 2q_0(q_1 i + q_2 j + q_3 k).$$

As $-1 \equiv 1\ (mod\, 2)$, $x^2 = x_s^2$.

Case 2. (p is an odd prime) As we see that if $x \in Id(\mathbb{H}/\mathbb{Z}_p)$, then $q_0 = \dfrac{p+1}{2}$ and $q_1^2+q_2^2+q_3^2 = \dfrac{p^2-1}{4}$. Also, if $x \in Id(\mathbb{H}/\mathbb{Z}_p)$, then $q_0 = \dfrac{p+1}{2}$ and $-q_1^2+q_2^2+q_3^2 = \dfrac{1-p^2}{4}$. From these equations it follows that $q_2^2 \equiv -q_3^2\ (mod\ p)$,

$$(q_2^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-2}{2}}(q_3^2)^{\frac{p-1}{2}}\ (mod\ p),$$

and

$$q_2^{p-1} \equiv (-1)^{\frac{p-1}{2}} q_3^{p-1}\ (mod\ p).$$

Using Fermat's Little Theorem we get $1 \equiv (-1)^{\frac{p-1}{2}}\ (mod\ p)$, but for $p = 4k+3$, we get $1 \not\equiv -1\ (mod\ p)$. So solution does not exist for $p \equiv 3\ (mod\, 4)$. For $p = 4k+1$, $1 \equiv 1\ (mod\, 4)$, so the solution exists only for $p \equiv 1\ (mod\, 4)$.

Let $-q_3^2 \equiv -q_2^2 = y\ (mod\ p)$. It is proved in [7] that $x^2 \equiv a\ (mod\ p)$ either has no solution or has exactly two solutions. If $p|y$, then $q_3 = 0\, (mod\ p)$ has exactly one solution. For each value of y, q_2 takes 2 values, so there are $2(p-1)$ possible solutions. Also, q_1 takes 2 values for each q_2 and q_3. So, $2\big(2(p-1)+1\big)+2 = 4p$. ■

3.2. Comparison of nilpotents

From Theorem 1.6 we get $q_1^2 - q_2^2 - q_3^2 = 0$ for an element nilpotent in $\mathbb{H}_s/\mathbb{Z}_p$ and $q_1^2+q_2^2+q_3^2 = 0$ in $\mathbb{H}/\mathbb{Z}_p$. Following tables give respectively the values q_1, q_2 and q_3.

Case 1. For $p = 2$,

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 0	0, 0, 0
0, 1, 1	0, 1, 1
1, 0, 1	1, 0, 1
1, 1, 0	1, 1, 0

Case 2. For $p = 3$

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 0, 0	0, 0, 0, 0
0, 1, 1, 1	0, 1, 0, 1
0, 1, 1, 2	0, 1, 0, 2
0, 1, 2, 1	0, 1, 1, 0
0, 1, 2, 2	0, 1, 2, 0
0, 2, 1, 1	0, 2, 0, 1
0, 2, 1, 2	0, 1, 0, 2
0, 2, 2, 1	0, 2, 1, 0
0, 2, 2, 2	0, 1, 2, 0

Case 3. For $p = 5$

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 0	0, 0, 0	0, 4, 3	0, 4, 3	2, 4, 0	2, 3, 0
0, 1, 2	0, 1, 2	1, 0, 2	1, 0, 1	3, 0, 1	3, 0, 2
0, 1, 3	0, 1, 3	1, 0, 3	1, 0, 4	3, 0, 4	3, 0, 3
0, 2, 1	0, 2, 1	1, 2, 0	1, 1, 0	3, 1, 0	3, 2, 0
0, 2, 4	0, 2, 4	1, 3, 0	1, 4, 0	3, 4, 0	3, 3, 0
0, 3, 1	0, 3, 1	2, 0, 1	2, 0, 2	4, 0, 2	4, 0, 1
0, 3, 4	0, 3, 4	2, 0, 4	2, 0, 3	4, 0, 3	4, 0, 4
0, 4, 2	0, 4, 2	2, 1, 0	2, 2, 0	4, 2, 0	4, 1, 0
				4, 3, 0	4, 4, 0

Following theorem gives common nilpotent elements in $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$.

Proof for Theorem 1.12. As for both $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$, nilpotency index is 2 and $q_0 = 0$.

Case 1. ($p = 2$) As $-1 \equiv 1\ (mod\ 2)$, so $x^2 = (x')^2$. In Theorem 1.8, for any prime p, the total number of nilpotent elements is p^2.

Case 2. (p is an odd prime) As we see that if $x \in nil(\mathbb{H}/\mathbb{Z}_p)$, then $q_1^2 + q_2^2 + q_3^2 = 0$. Also, if $x \in nil(\mathbb{H}_s/\mathbb{Z}_p)$, then $q_1^2 - q_2^2 - q_3^2 = 0$. Comparing these relations, we arrive at $q_2^{p-1} \equiv (-1)^{\frac{p-1}{2}} q_3^{p-1}\ (mod\ p)$. The solution exists only for $p \equiv 1\ (mod\ 4)$. Now, for each value of y, q_2 takes 2 values, and so there are $2(p-1)$ possible solutions. Finally, we get $2(p-1) + 1 = 2p - 1$. ∎

3.3. Comparison of zero divisors

By using the above codes we can easily find all zero divisors in $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$ for $p = 3, 5, 7$.

Case 1. (When $p = 2$)

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 0, 0	0, 0, 0, 0
0, 0, 1, 1	0, 0, 1, 1
0, 1, 0, 1	0, 1, 0, 1
0, 1, 1, 0	0, 1, 1, 0
1, 0, 0, 1	1, 0, 0, 1
1, 0, 1, 0	1, 0, 1, 0
1, 1, 0, 0	1, 1, 0, 0
1, 1, 1, 1	1, 1, 1, 1

Case 2. (When $p = 3$) $x, y \in Zd(\mathbb{H}/\mathbb{Z}_p) \cap Zd(\mathbb{H}_s/\mathbb{Z}_p)$ if and only if $xy = q_0^2 + q_1^2 + q_2^2 + q_3^2$ and $xy = q_0^2 + q_1^1 - q_2^2 - q_3^2$. The following table respectively shows the values of q_0, q_1, q_2, and q_3 which satisfy the above relations in $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$.

$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$	$\mathbb{H}/\mathbb{Z}_p$	$\mathbb{H}_s/\mathbb{Z}_p$
0, 0, 0, 0	0, 0, 0, 0	1, 2, 0, 2	1, 0, 1, 0	2, 0, 1, 2	2, 0, 0, 2
0, 1, 1, 1	0, 1, 0, 1	1, 2, 1, 0	1, 0, 2, 0	2, 2, 0, 2	2, 0, 1, 0
0, 1, 1, 2	0, 1, 0, 2	1, 0, 2, 1	1, 1, 1, 1	2, 2, 1, 0	2, 0, 2, 0
0, 1, 2, 1	0, 1, 1, 0	1, 0, 2, 2	1, 1, 1, 2	2, 0, 2, 1	2, 1, 1, 1
0, 1, 2, 2	0, 1, 2, 0	1, 1, 0, 1	1, 1, 2, 1	2, 0, 2, 2	2, 1, 1, 2
0, 2, 1, 1	0, 2, 0, 1	1, 1, 0, 2	1, 1, 2, 2	2, 1, 0, 1	2, 2, 2, 2
0, 2, 1, 2	0, 1, 0, 2	1, 1, 1, 0	1, 2, 1, 1	2, 1, 0, 2	2, 1, 2, 1
0, 2, 2, 1	0, 2, 1, 0	1, 1, 2, 0	1, 2, 1, 2	2, 1, 1, 0	2, 1, 2, 2
0, 2, 2, 2	0, 1, 2, 0	1, 2, 0, 1	1, 2, 2, 1	2, 1, 2, 0	2, 2, 1, 1
1, 0, 1, 1	1, 0, 0, 1	1, 2, 2, 0	1, 2, 2, 2	2, 2, 0, 1	2, 2, 1, 2
1, 0, 1, 2	1, 0, 0, 2	2, 0, 1, 1	2, 0, 0, 1	2, 2, 2, 0	2, 2, 2, 1

The following is the proof of number of zero divisors that are common in $\mathbb{H}_s/\mathbb{Z}_p$ and $\mathbb{H}/\mathbb{Z}_p$.

Proof for Theorem 1.13. As we already know that if for $x \in \mathbb{H}/\mathbb{Z}_p$, then $N(x) = x\overline{x} = q_0^2 + q_1^2 + q_2^2 + q_3^2$. Similarly, for $x \in \mathbb{H}_s/\mathbb{Z}_p$, $N(x) = x\overline{x} = q_0^2 + q_1^2 - q_2^2 - q_3^2$.

Case 1. (When $p = 2$) Since $-1 \equiv 1$ $(mod\ p)$, $|Zd(\mathbb{H}/\mathbb{Z}_p)| = |Zd(\mathbb{H}_s/\mathbb{Z}_p)| = p^3$.

Case 2. (When p is an odd prime) From the above two relations, we have $q_2^2 + q_3^2 = -q_2^2 - q_3^2$ $(mod\ p)$ and $q_2^2 + q_2^3 = 0$ $(mod\ p)$. As $p \equiv 3$ $(mod\ 4)$, the above relation has no solution. For $p \equiv 1$ $(mod\ 4)$, it has $2p - 1$ solutions. Now, if $q_2^2 + q_3^2 = 0$, then the sum of squares of q_0 and q_1 must be 0, and hence has $2p - 1$ solutions. The total count is $(2p - 1)^2$. ■

Remark 3.1. The present work can be extended to algebras of octonians and split octonians over $\mathbf{Z}_p$.

4. Appendix

Here we give codes in software C^{++} to find the idempotents, nilpotents and zero divisors in $\mathbb{H}/\mathbb{Z}_p$ and $\mathbb{H}_s/\mathbb{Z}_p$. In the next section these codes will play an important role to list these elements in both types of algebras.

4.1. A Word in Computer Language

Code for $\mathbb{H}/\mathbb{Z}_p$
$include < iostream >$
Using name space std;
int main(){
int p;
int q_1, q_2, q_3;
int sum;

```
int n;
int count= 2, totalCount= 0;
cout<<"Enter value for p:";cin>>p;
n = (p * p − 1)/4;
while(n≥p)
n = n%p
cout<<"value of n is:"<<n<<endl;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
sum= q1 * q1 + q2 * q2 + q3 * q3;
while(sum<0)
sum = sum+p;
ifp(sum% == n){
count++;
cout<<q1<<" "<<q2<<" "<<q3<<endl;
} } } }
cout<<"Total Count is:"<<totalCount<<endl;
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

Code for $\mathbb{H}_s/\mathbb{Z}_p$

```
include < iostream >
Using name space std;
int main(){
int p;
int q1, q2, q3;
int sum;
int n;
int count= 2, totalCount= 0;
cout<<"Enter value for p:";cin>>p;
n = (1 − p * p)/4;
while(n<0)
n = n + p
cout<<"value of n is:"<<n<<endl;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
```

```
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
sum= −q1 ∗ q1 + q2 ∗ q2 + q3 ∗ q3;
while(sum<0)
sum = sum+p;
ifp(sum% == n){
count++;
cout<<q1<<" "<<q2<<" "<<q3<<endl;
}
}
}
}
cout<<"Total Count is:"<<totalCount<<endl;
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

4.2. Nilpotents

Code for $\mathbb{H}/\mathbb{Z}_p$

```
include < iostream >
Using name space std;
int main(){
int p;
int q1, q2, q3;
int sum;
int n;
int count= 0, totalCount= 0;
cout<<"Enter value for p:";cin>>p;
n = 0;
while(n≥p)
n = n%p
cout<<"value of n is:"<<n<<endl;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
```

```
sum= q1 * q1 + q2 * q2 + q3 * q3;
while(sum<0)
sum = sum+p;
ifp(sum% == n){
count++;
cout<< q1 <<" "<< q2 <<" "<< q3 <<endl;
}
}
}
}
cout<<"Total Count is:"<<totalCount<<endl;
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

Code for $\mathbb{H}_s/\mathbb{Z}_p$

```
include < iostream >
Using name space std;
int main(){
int p;
int q1, q2, q3;
int sum;
int n;
int count= 0, total Count= 0;
cout<<"Enter value for p:";cin>>p;
n = 0;
while(n>0)
n = n%p
cout<<"value of n is:"<<n<<endl;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
sum= −q1 * q1 + q2 * q2 + q3 * q3;
while(sum<0)
sum = sum+p;
ifp(sum% == n){
count++;
cout<< q1 <<" "<< q2 <<" "<< q3 <<endl;
}
```

```
}
}
}
cout<<"Total Count is:"<<totalCount<<endl;
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

4.3. Zero Divisors

Code for $\mathbb{H}/\mathbb{Z}_p$

```
include < iostream >
Using name space std;
int main(){
int p;
int q0, q1, q2, q3;
int sum;
int n;
int count= 0, totalCount= 0;
cout<<"Enter value for p:";cin>>p;
n = 0;
while(n≥p)
n = n%p
cout<<"value of n is:"<<n<<endl;
for(inth = 0; h < p; h++){
q0 = h;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
sum= q0 * q0 + q1 * q1 + q2 * q2 + q3 * q3;
while(sum<0)
sum = sum+p;
if p(sum% == n){
count++;
cout<< q0 <<" "<< q1 <<" "<< q2 <<" "<< q3 <<endl;
}
}
}
```

```
}
}
cout<<"Total Count is:"<<totalCount<<endl;
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

Code for $\mathbb{H}_s/\mathbb{Z}_p$

```
include < iostream >
Using name space std;
int main(){
int p;
int q0, q1, q2, q3;
int sum;
int n;
int count= 0, total Count= 0;
cout<<"Enter value for p:";cin>>p;
n = 0;
while(n>0)
n = n%p
cout<<"value of n is:"<<n<<endl;
for(inth = 0; h < p; h++){
q0 = h;
for(inti = 0; i < p; i++){
q1 = i;
for(inti = 0; j < p; j++){
q2 = j;
for(intk = 0; k < p; k++){
q3 = k;
totalCount++;
sum= q0 * q0 + q1 * q1 − q2 * q2 − q3 * q3;
while(sum<0)
sum = sum+p;
ifp(sum% == n){
count++;
cout<< q0 <<" "<< q1 <<" "<< q2 <<" "<< q3 <<endl;
}
}
}
}
}
cout<<"Total Count is:"<<totalCount<<endl;
```

```
cout<<"Count is:"<<count<<endl;
system("pause");
return 0;
}
```

References

[1] Y. Alagöz, K. H. Oral and S. Yüce S, Split quaternion matrices, Miskolc Mathematical Notes, **13** (2012), pp. 223–232.

[2] M. Aristidou, Idempotent elements in quaternion rings over $\mathbb{Z}_p$, Int. J. Algebra, **6** (2012), pp. 249–254.

[3] M. Aristidou, A note on nilpotent elements in quaternion rings over $\mathbb{Z}_p$, Int. J. Algebra, **6** (2012), pp. 663–666.

[4] M. Aristidou and A. Demetre, A Note on Quaternion Rings over $\mathbb{Z}_p$, Int. J. Algebra, **3** (2009), pp. 725–728.

[5] J. C. Baez, Errata for: "The octonions" [Bull. Amer. Math. Soc. (N.S.) 39 (2002), 145-205]. Bull. Amer. Math. Soc. (N.S.), **42** (2005), p. 213.

[6] D. C. Brody and E. M. Graefe, On complexified mechanics and coquaternions. J. Phys. A, Math. Theor., **44** (2011), 072001.

[7] D. M. Burton, Elementary Number Theory, Allyn and Bacon, Inc., Boston, 1980.

[8] J. Cockle, On systems of algebra involving more than one imaginary, Philosophical Magazine (series 3), **35** (1849), pp. 434–435.

[9] J. H. Conway and D. A. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, Bull. Amer. Math. Soc., **42** (2005), pp. 229–243.

[10] M. Erdoğdu and M. Özdemir, On eigenvalues of split quaternion matrices. Adv. Appl. Clifford Algebras, **23** (2013), pp. 615–623.

[11] N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent, Illinois J. Math., **2** (1958), 499–504.

[12] I. Frenkel and M. Libine, Split quaternionic analysis and separation of the series for $SL(2,\mathbb{R})$ and $SL(2,\mathbb{C})/SL(2,\mathbb{R})$. Adv. Math., **228** (2011), pp. 678–763.

[13] J. Inoguchi, Timelike surfaces of constant mean curvature in Minkowski 3-space, Tokyo J. Math., **21** (1998), 141–152.

[14] J. Inoguchi and M. Toda, Timelike minimal surfaces via loop groups, Acta Appl. Math., **83** (2004), pp. 313–355.

[15] L. Kula and Y. Yayli, Split quaternions and rotations in semi Euclidean space $\mathbb{E}_2^4$, J. Korean Math. Soc., **44** (2007), pp. 1313–1327.

[16] C. J. Miguel and R. Serôdio, On the structure of quaternion Rings over $\mathbb{Z}_p$, Int. J. Algebra, **5** (2011), pp. 1313–1325.

[17] M. Özdemir, The roots of a split quaternion, Appl. Math. Lett., **22** (2009), pp. 258–263.

[18] M. Özdemir and A. A. Ergin, Some geometric applications of split quaternions, in: Proc. 16th Int. Conf. Jangjeon Math. Soc., 108-115, Jangjeon Math. Soc., Hapcheon, 2005.

[19] M. Özdemir and A. A. Ergin, Rotations with timelike quaternions in Minkowski 3-space, J. Geom. Phys., **56** (2006), pp. 322–336.